



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/680,258	10/05/2000	Junichi Kokudo	Q61120	8838

7590 12/17/2003

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue N.W.
Washington, DC 20037

EXAMINER

MCLoughlin, Michael I

ART UNIT

PAPER NUMBER

2662

DATE MAILED: 12/17/2003

2

Please find below and/or attached an Office communication concerning this application or proceeding.

TS

Office Action Summary

Application No.

09/680,258

Applicant(s)

KOKUDO, JUNICHI

Examiner

Michael I McLoughlin

Art Unit

2662

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on _____.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-11 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 05 October 2000 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) The translation of the foreign language provisional application has been received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
- 4) Interview Summary (PTO-413) Paper No(s). _____ .
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____ .

1) Claim Rejections - 35 USC § 112

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant's admitted prior art, hereinafter referred to as APA, and further in view of Lewis (U.S. 6,453,159), hereinafter referred to as Lewis..

Regarding claim 1, APA teaches a *conventional* authentication method as shown in figure 2 at a wireless LAN system as shown in figure 1, comprising the steps of:

- transmitting an authentication request from a STA to an AP, with which said STA desires to make association (S1 of figure 2);
- *requesting authentication of said authentication request from said AP (authentication request to AP, S1 of figure 2)*
- *checking said authentication request at said AP based on a MAC (media access control) address of said STA (S5 of figure 2 and MAC address authentication function on lines 25-26 of page 1 in the specification);*
- *executing encryption authentication at said AP with said STA based on a designated encryption algorithm (executing encryption at S3 of figure 2 based on WEP); and*
- *notifying an authentication completion from said STA to said AP.*
- *notifying an authentication completion from said AP.*

APA fails to teach an application server and the relationship between the AP and the application server. Lewis teaches an authentication server (key distribution server 76) as shown in figure 1 that interoperates with APs 54 of figure 1 to add a second encryption layer for additional security that modifies the *conventional steps* above as follows:

- requesting authentication of said authentication request from said AP to an authentication server (the STA authentication request received at the AP is passed to the back bone at step 224 of figure for processing of the second layer by the key distribution server), by converting said authentication request to a protocol adaptable to said authentication server (converting the authentication request to a two layer encryption adapted for the key distribution server 76);
- checking said authentication request at said authentication server based on a MAC (media access control) address of said STA (checking the authentication request at the key distribution server 76 at step 252 of figure 8 against the system device table 152 of figure the where the authorized device ID, which inherently includes a MAC address taught by the APA and IEEE 802.11 taught by Lewis in lines 12-13 of column 6);
- executing encryption authentication at said AP (executing step 222 of figure 7) with said STA based on a designated encryption algorithm; and
- notifying an authentication completion from said authentication server to said AP (authentication completion by the key distribution server at step 262 of figure 8 appropriately by sending a message to the AP and received and determined by the AP at step 282 of figure 9), after said authentication server received a response of a completion of said encryption

authentication from said AP (after Key distribution server 76 receives a forwarded message from the AP at step 224 based on step 222 of figure 7, and see lines 53-54 of column 14).

3. Regarding claim 2, Lewis further teaches an authentication method at a wireless LAN system shown in figure 1 in accordance with claim 1, wherein:

- after said encryption authentication is normally completed, a table of said MAC address in said AP is renewed by an instruction from said authentication server (clear table 126 in the AP taught in lines 36-40 of column 3 is periodically updated by the key distribution server 76 as taught in step 250 of figure 8).

4. Regarding claim 3, Lewis further teaches an authentication method at a wireless LAN system in accordance with claim 1, wherein:

- in case that a trouble occurs at said authentication server, said AP itself executes authentication of said MAC address (the examiner interprets Lewis's method and apparatus as being consistent with the common philosophies of maximizing network up time, minimizing down time, and especially avoiding total network outages. With this interpretation should the key distribution server fail 76, the AP will fall back to conventional techniques for authentication with the STAs, see line 43 of column 4, have the first layer of protection, and await the recovery of the key distribution server to recover the second layer protection>)

Art Unit: 2662

5. Regarding claim 4, Lewis further teaches an authentication method at a wireless LAN system in accordance with claim 1, wherein:

- said encryption algorithm uses a shared key having a predetermined usable period (shared keys are used at the STA and APS as taught in figure 2, and at the key distribution server 76 as taught in figure 3, and these keys have a period of usage as taught in the access expiration column of figure 4, and also taught as time limits in line 29 of column 10).

6. Regarding claim 5, APA teaches an authentication method at a wireless LAN system in accordance with claim 4, wherein:

- a MAC address is authenticated by an open system authentication method in line 8 of the specification; and
- in the open authentication method it is inherent that a key is transported using an Internet Key Exchange method of Public Key Infrastructure.

APA fails to teach limiting the time for the use of a shared key or reestablishing a shared key when the predetermined useable period of said shared key expires.

Lewis further teaches:

- in case that said predetermined usable period of said shared key expired, said MAC address is authenticated by an open system authentication method (a shared key is limited in time as cited above in claim 4 in the case that the usable period of said shared key expired the AP would decide NO at step 222 proceed to step 226 and find the source included in the clear table and decide yes and pass this to the key distribution server 76 via step 224 in figure 7) ; and

Art Unit: 2662

- at said open system authentication method, after association, a period of communication is limited to a designated short time, and a key is transported in said limited time by using such an Internet Key Exchange method of Public Key Infrastructure, and said authentication request is executed again by using said shared key (key distribution server 76 on receipt of the message from the AP executed at step 224 of figure 7 and would decide yes at step 252 then go to step 254 and decide yes, and then transmit a shared key to the requesting device at step 256 of figure 8 .

It would have been obvious to one of ordinary skill in the art to modify APA's *conventional* authentication method with the teaching of Lewis and arrive at the claimed invention. One would have been motivated to make this modification in order to maintain a *conventional* authentication method and network integrity between the STA and the AP (see lines 49-51 of column 2) while adding additional security to overcome the potential unauthorized or compromising use of the network taught by Lewis in lines 58 of column 1 through line 14 of column 2.

7. Regarding claim 6, APA teaches an authentication apparatus at a wireless LAN system in figures 1 and 2, comprising:

- plural STAs 1 of figure 1; and
- plural APs 2 of figure 1

APA fails to teach an application server and the relationship between the AP and the application server. Lewis teaches an authentication server (key distribution server 76) as shown in figure 1

Art Unit: 2662

that interoperates with APs 54 of figure 1 to add a second encryption layer for additional security that modifies the apparatus above as follows

- plural APs which connect to an authentication server and said plural STAs, and one of said plural APs receives an authentication request from one of said plural STAs (the STA authentication request received at the AP is passed to the back bone at step 224 of figure for processing of the second layer by the key distribution server) and converts said authentication request from one of said plural STAs to a protocol adaptable to said authentication server (converting the authentication request to a two layer encryption adapted for the key distribution server 76), and authenticates said authentication request from one of said plural STAs based on a designated encryption algorithm (AP executes step 222 of figure 7 and authenticates by deciding YES); and
- said authentication server which checks said authentication request from one of said STAs based on a MAC address of one of said plural STAs by receiving said converted authentication request (checking the authentication request at the key distribution server 76 at step 252 of figure 8 against the system device table 152 of figure the where the authorized device ID, which inherently includes a MAC address taught by the APA and IEEE 802.11 taught by Lewis in lines 12-13 of column 6, and), and notifies an authentication completion to said AP (authentication completion by the key distribution server at step 262 of figure 8 appropriately by sending a message to the AP and received and determined by the AP at step 282 of figure 9), after said authentication server received a response of a completion of encryption authentication from said AP (after Key

distribution server 76 receives a forwarded message from the AP at step 224 based on step 222 of figure 7, and see lines 53-54 of column 14)

8. Regarding claim 7, Lewis further teaches an authentication apparatus at a wireless LAN system shown in figure 1 in accordance with claim 6, wherein:

- after said encryption authentication is normally completed, a table of said MAC address in said AP is renewed by an instruction from said authentication server (clear table 126 in the AP taught in lines 36-40 of column 3 is periodically updated by the key distribution server 76 as taught in step 250 of figure 8).

9. Regarding claim 8, Lewis further teaches an authentication apparatus at a wireless LAN system in accordance with claim 6, wherein:

- in case that a trouble occurs at said authentication server, said AP itself executes authentication of said MAC address (the examiner interprets Lewis's method and apparatus as being consistent with the common philosophies of maximizing network up time, minimizing down time, and especially avoiding total network outages. With this interpretation should the key distribution server fail 76, the AP will fall back to conventional techniques for authentication with the STAs, see line 43 of column 4, have the first layer of protection, and await the recovery of the key distribution server to recover the second layer protection>)

10. Regarding claim 9, an authentication apparatus at a wireless LAN system in accordance with claim 6, wherein:

- said authentication algorithm is a WEP (wired equivalent privacy) algorithm stipulated in the IEEE 802.11 (Lewis teaches WEP protocol in an IEEE802.11 standard, see lines 58-59 of column 6).

11. Regarding claim 10, Lewis further teaches an authentication apparatus at a wireless LAN system in accordance with claim 1, wherein:

- said encryption algorithm uses a shared key having a predetermined usable period (shared keys are used at the STA and APS as taught in figure 2, and at the key distribution server 76 as taught in figure 3, and these keys have a period of usage as taught in the access expiration column of figure 4, and also taught as time limits in line 29 of column 10).

12. Regarding claim 11, APA teaches an authentication apparatus at a wireless LAN system in accordance with claim 4, wherein:

- a MAC address is authenticated by an open system authentication method in line 8 of the specification; and
- in the open authentication method it is inherent that a key is transported using an Internet Key Exchange method of Public Key Infrastructure.

It would have been obvious to one of ordinary skill in the art to modify APA's authentication method with the teaching of Lewis and arrive at the claimed invention. One would have been

Art Unit: 2662

motivated to make this modification in order to maintain an existing authentication apparatus and network integrity between the STA and the AP (see lines 49-51 of column 2) and have no additional hardware cost associated while adding additional security to overcome the potential unauthorized or compromising use of the network taught by Lewis in lines 58 of column 1 through line 14 of column 2.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- 1) Lewis (U.S. 6,526,506), Multi-level encryption access point for wireless network.
- 2) Wu et al. (U.S. 6,332,077), Intelligent roaming in AGC application.
- 3) Gernert et al. (U.S. 6,600,734), Apparatus for interfacing a wireless local network and a wired voice telecommunications.
- 4) Chuah et al. (U.S. 6,400,722), Optimum routing system,
- 5) Harrison et al. (U.S. 5,796,727), Wide-area wireless LAN access.
- 6) Bellare et al. (U.S. 5,673,318), Method and apparatus for data authentication in a data communication environment.
- 7) Hsu (U.S. 6,345,043), Access scheme for a wireless LAN station to connect an access point.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael I McLoughlin whose telephone number is 703-308-7911. The examiner can normally be reached on weekdays 7AM - 3:30PM.

Art Unit: 2662

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on 703-305-4744. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-4700.

MIM
December 12, 2003



HAZZAN KIZOU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600